State of Wisconsin

AND

HIPAA Compliance

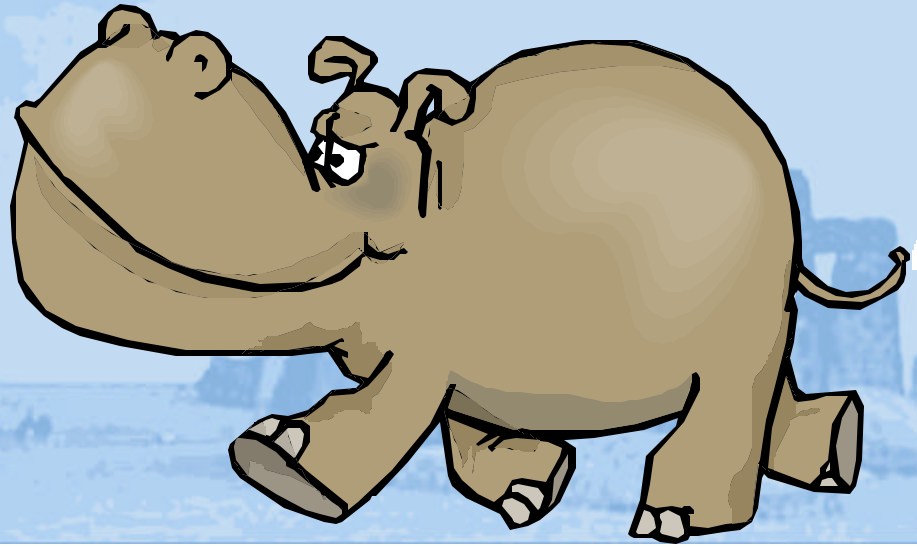
Health Insurance Portability and Accountability Act (HIPAA)

Jack Hough

Developed by

StoneHenge PARTNERS, INC.

Attend the 2:45 - 3:30 Breakout Sessions for Ground Zero to Compliance Guidelines



StoneHenge
PARTNERS, INC.

HIPAA Ground Zero (Assessment) Breakdown

- **Starting at Ground Zero (*HIPAA Assessment*)**
  - **Performing a HIPAA Assessment or Audit**
- **Step 1 – Develop a HIPAA Task Force**
- **Step 2 – HIPAA Education and Awareness**
- **Step 3 - Performing a GAP Analysis**
- **Step 4 – Develop Working Strategies for Compliance**
- **Step 5 – Develop Working Plans for Compliance**

Processes for HIPAA Compliance Guide

- **Step 1 – Develop a HIPAA Task Force**
  1. **Establish the Purpose of the Task Force**
     - **A. To Guide the HIPAA Process**
     - **B. Make Critical Decisions**
     - **C. Prepare Audit Trail Process**
     - **D. HIPAA Compliance Planning**
     - **E. Define What is Reasonable**
  2. **Obtain Executive Level Involvement**
  3. **Assemble a Team of Key Personnel**
  4. **Assign Responsibility to Team Members**
  5. **Develop a Forum for HIPAA Discussions**
  6. **Establish Meeting Schedules**

Processes for HIPAA Compliance Guide

- **Step 2 - HIPAA Education and Awareness Programs**
  - **Develop a HIPAA Awareness Program**
    - **Identify the HIPAA Questions that are circulating in your organization and address them.**
    - **Explain the basics of HIPAA**
      - **What is HIPAA?**
      - **Why HIPAA?**
      - **What Does HIPAA Do?**
      - **How Will HIPAA Impact Us?**
      - **How Much Will HIPAA Cost?**
      - **When and What Do We Need to Do?**
      - **What are the Penalties?**
    - **Continuing Education**
      - **Be HIPAA Aware**
      - **Daily Operations and HIPAA**

Processes for HIPAA Compliance Guide

- **Step 3 – Performing a GAP Analysis**
  - ***(Determining the GAP's in your organizations HIPAA readiness)***

  - **HIPAA Privacy Analysis**
  - **HIPAA Security Analysis**
  - **HIPAA Standardization Analysis**

Processes for HIPAA Compliance Guide

- **Performing a GAP Analysis**
  - ***(Determining the GAP's in your organizations HIPAA readiness)***
  - **Document the current activities, processes, practices, policies, and procedures, and rate the level of GAP between the organization level and the HIPAA requirements.**
  - **Using a High, Medium, and Low for measurement**
  - **Assess the Risk to the organization by taking the level of GAP (High – Low) and the weight of the HIPAA Requirement and rank the Risk.**
  - **Using High, Medium, and Low for measurement**

HIPAA GAP Analysis Example

Compliance Requirement	Gap	Summary of Risk & Required Action	Risk
AP.2 - Business Associate Agreements			
A review of all Business Associate exchanges has been completed to determine extent of access to data. The appropriate Business Associate agreements are in place.	HIGH	There are no Business Associate contracts in place at this time that approriately delineate the transmission, receipt, storage and processing requirements of the Security and Privacy Regulations.	HIGH
AP.3 - Contingency Planning			
A fully documented contingency plan for system emergencies is in place. The organization is performing regular backups, have back-up facilities available in the event of an emergency and disaster recovery procedures are in place.	MED	There is no documented Contingency Plan in place at this time. While there is a Disaster Recovery Plan for a primary Business Associate, a corresponding detailed plan must be created for this site. This site has contracted for the planning effort necessary to create the project plan for such a Contingency Plan.	LOW

This entity did not have a Business Associate Agreement in place making the GAP High, and the Risk also High. The entity had only a DR Plan, but no documented Contingency Plan, making the GAP only Medium, but the Risk Low.

Example HIPAA Questionnaire Example

Develop questions from the Regulations to assist in data gathering

Organization: StoneHenge Partners Inc. Department:

HIPAA Compliance Survey and Review

Business Impact Analysis Questions	BIA Result (Yes/No)	GAP Analysis (See Rating Chart)	Risk Analysis (High, Medium or Low)	Impact Significance (High, Medium or Low)	Person Interviewed	Document Type (Name)	Sample Document (Yes/No)	Comments (Use Comments column as needed to explain any answer)
Chain of Trust Partner Agreements								
If your organization have data that is processed through a third party, the parties would be required to enter into a chain of trust agreement. This is a contract in which the parties agree to electronically exchange data and to protect the transmitted data. The sender and receiver are required and depend upon each other to maintain the integrity and confidentiality of the transmitted information. Multiple two-party contracts may be involved in moving information from the originating party to the ultimate receiving party. These agreements are important so that the same level of security will be maintained at all links in the chain when information moves from one organization to another.								
Has published policies and procedures been developed for Chain of Trust Partner Agreements?								
Has legal counsel developed and/or reviewed contract language for your chain of trust partner agreements?								
Has a process been established to identify all parties in the chain of trust contracts including:								
agents/contractors/volunteers/students accessing personally identifiable health information?								
coding vendor contracts?								
computer hardware contracts?								
computer software contracts?								
data warehouse/clearinghouse vendor contracts?								
emergency services contracts?								
employment contracts?								
hospitalist contracts?								
insurance contracts?								

Performing A GAP Analysis - Privacy

- **Privacy Provisions**
  - **Designating a Privacy Official**
- **Use and Disclosure**
  - **The conditions that permits the limited use and disclosure are covered under Treatment and Payment and Operations.**
- **Patient's Rights**
  - **Right to request or obtain, amend or object to listed information, and obtain an accounting of disclosures**
  - **Restricted uses and disclosures**

Performing A GAP Analysis - Privacy

- **Minimum Necessary**
  - **Is the practice of only giving specific data and having limited access (*to accomplish the intended purpose*) to patient health information.**
- **Notice of Privacy Practices**
  - **The informing to patients of how their information will be used, disclosed, and kept confidential along with the individuals rights and the covered entities legal responsibilities**
- **Modifications to Privacy Regulations**
  - **Monitoring Changes**
  - **New Regulations**

Performing A GAP Analysis - Privacy

- **HIPAA Privacy Analysis**
  - **Identify and Review Privacy Notices, Consents, Authorizations, and Business Associate Agreements for appropriate language Privacy Policy and Procedures.**
    - **Identify and Review Practices, Policies and Procedures pertaining to the following: (*Not Inclusive*)**
      - **Permitted Use and Disclosures of any kind**
      - **Minimum Necessary**
      - **Whistleblower Disclosures**
      - **Business Associate Disclosures**
      - **Obtaining of Consent**
      - **Revocation of Consent**
      - **Obtaining of Authorization**

Performing A GAP Analysis - Privacy

- **Administrative Requirement**
  - **Personnel Designations**
    - **Identify the designated Privacy Official who is responsible for the development and implementation of the policies and procedures of the entity.**
    - **Identify and review the designated contact and processes that provide for the receiving of complaints.**
    - **Identify and review personnel job descriptions**
  - **Training**
    - **Identify and review the privacy training program and associated documentation for training completion.**

Performing A GAP Analysis - Privacy

- **Administrative Requirement (*Continued)***
  - **Safeguards**
    - **Identify and review the administrative, technical and physical safeguards to protect the privacy of protected health information.**
    - **Identify and review if current safeguards are "reasonable" to protect information from intentional or unintentional use or disclosure.**
  - **Sanctions**
    - **Identify and review the privacy sanctions policy and procedures**
  - **Change Process**
    - **Identify and review the entity's policy and procedure change process.**

Performing A GAP Analysis - Security

- **HIPAA Security Analysis (*Review*)**
  - **Administrative Procedures**

Documented, formal practices to manage the selection and execution of security measures to protect data, and to mange the conduct of personnel in relation to the protection of data.

- **Business Continuity Planning (*Contingency Planning*)**
- **Review current security practices, policies, procedures, measures, and written security, and internal audit plans.**
- **Review Chain of Trust Agreements**
- **Determine if all personnel who have access to sensitive data have the authority and clearances**
- **Review the Security Training program**
- **Document the compliance level vs. the HIPAA requirement and rank accordingly.**

Performing A GAP Analysis - Security

- **Physical Safeguards**

  Protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion.

  - **Identify who is assigned the responsibility to manage and supervise the execution and use of security measures.**
  - **Review formal (*documented*) policies and procedures for Media Controls (receipt and removal of *hardware / software)***
  - **Review formal (*documented*) policies and procedures that control physical access (limited, but appropriate access)**
  - **Review documented procedures on guidelines for workstation use.**
  - **Review the physical safeguards for secure workstation locations**
  - **Review the Security Awareness Training all employees must participate in for adequacy.**
  - **Document the compliance level vs. the HIPAA requirements and rank accordingly.**

Performing A GAP Analysis – Security

- **Technical Security Services**

  The processes that are put in place to protect information and to control individual access to information.

  - **Identify and review the processes that are put into place to protect information.**
  - **Identify and review the processes that are put into place to control access to information.**
  - **Identify and review the processes that are utilized to corroborate that data has not been altered or destroyed.**
  - **Identify and review the processes that are utilized to corroborate an entity is the one it claims to be.**
  - **Document the compliance level vs. the HIPAA requirement and rank accordingly.**

Performing A GAP Analysis - Security

- **Technical Security Mechanisms**

  Processes that are put in place to guard against unauthorized access to data that is transmitted over a communications network.

  - **Review mechanisms and processes that are put in place to guard against unauthorized access to data over a network.**
  - **Review Network Security Controls.**
  - **Review Network Access Controls.**
  - **Review processes for message authentication.**
  - **Review Network Event and Alarm logs for events reported.**
  - **Review Network Audit Trials**
  - **Document the compliance level vs. the HIPAA requirement and rank accordingly.**

Performing A GAP Analysis - Security

- **Electronic Signature (*Optional*)**

  A "digital signature" is an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters so that the identity of the signer and the integrity of the data can be verified.

  - **Review the use of electronic signatures**
  - **Review if the signature method in use can assure the unaltered transmission and receipt of a message from the sender to the intended recipient.**
  - **Review if the message integrity, is sufficient to prevent a party from denying the origin, submission, or delivery of the message and the integrity of the contents.**
  - **Review if an entity can be assured of the claimed identity.**
  - **Document the compliance level vs. the HIPAA requirement and rank accordingly.**

Performing a GAP Analysis - Standardization

3. Standardization and Code Set Analysis (*Review*)

- Identify Third Party Packages and/or Translators in use
  - Are they complaint?
  - Do they intend to release a compliant version and when?
  - If they do not intend to become compliant, what new vendor can take their place?
- Identify any In-House Code in use
  - Identify codes currently in use and the HIPAA replacements
  - Identify all programs /applications / processes that pass or create transactions
- Document the Compliance Level vs. the HIPAA Requirements and Rank Accordingly

HIPAA Transactions

Electronic Transaction Standards	ASC X12N, HL7 ✓
Standard Code Sets	ICD-10, CPT, HCPCS ✓
Employer Identifiers	Tax ID ✓
Health Plan Identifier	Payer ID
Individual Identifier	Proposed Controversial
Provider Identifiers	New—Alphanumeric ✓
Security and Electronic Signature	Not-Finalized
Privacy	Final Rule ✓
Claims Attachments	Work-in-Progress

Working Strategies

- **Step 4 – Developing Working Strategies for Compliance**
  - **Correlate the GAP and Risk Analysis and prioritize on the most risk and GAP to the lowest.**
  - **Research the GAP's for ways to reduce the risk**

    (Reducing the GAP, reduces the risk)
  - **Develop working options to correct the GAP's**
  - **Determine if the working options are feasible and costs to incurred**
  - **Document and Recommend working strategies for:**
    - **Privacy**
    - **Security**
    - **Standardization**

Working Strategies - Privacy

Document and Recommend working strategies for Privacy:

- **Defining what is Reasonable for the Organization**
- **Developing Polices and Procedures from GAP**
- **Developing Privacy Notices and Practices from GAP**
- **Defining permitted Uses and Disclosures (*TPO*)**
- **Defining Minimum Necessary**
- **Developing Business Associate Contracts**
- **Developing Authorizations or Consent forms**
- **Designate Privacy Officer**
- **Privacy Training**

Working Strategies - Security

Document and Recommend working strategies for Security:

- **Defining what is Reasonable for the Organization**
- **Developing Polices and Procedures from GAP**
- **All Physical and Data safeguards are adequate**
- **Written Security Plans exist**
- **Define Chain of Trust Partnership Agreements**
- **Protection of the system and information is maintained**
- **Develop Contingency plans**
- **Establish controls for communications**
- **Physical Safeguards exist**
- **Assign Security Officer**
- **Defined Media Controls are in Place**
- **Secure facilities and work areas**
- **Security Training**

Working Strategies - Standardization

Document and Recommend working strategies for Standardization:

- **Defining what is Reasonable for the Organization**
- **Vendor Compliance**
- **Identify new vendors or software**
- **Review and update vendor transaction translators**
- **Define migration content and schedule**
- **Map data fields in the new transaction codes to in-house database**
- **Update program logic to format new transactions**
- **Unit and system testing to ensure logic work as designed**
- **Coordinate test with trading partners**
- **Define production schedule dates for implementation**

Working Plans

- **Step 5 – Develop Working Plans for Compliance**
  - **Develop Implementation tasks from the working strategies.**
  - **Determine a time frame for completing the tasks**
  - **Identify personnel to complete the tasks**
  - **Evaluate the time frame, personnel, and costs.**
  - **Assemble the working plans into a single Implementation plan (*MS Project*)**

HIPAA Implementation (Remediation) Breakdown

- **Step 1 – Validating GAP Strategies**
- **Step 2 – Formalizing Compliance Plans**
- **Step 3 - Identification of Implementation Team**
- **Step 4 – Implementation of Task**
- **Step 5 – Internal Certification**

HIPAA Implementation (Remediation)

- **Implementation**

  Step 1 - Validating Working Strategies

  - **Identify if any assumptions, requirements, GAP's, or risk has changed.**
  - **Review timeframes for completing each strategy.**
  - **With the given timeframes do the current strategies meet the objective of reducing the GAP's and Risk?**
  - **Make preparations for HIPAA Implementation Budgets.**

  Step 2 - Formalizing Compliance Plans

  - **Review Implementation tasks to be done; are all strategies covered?**
  - **Establish a start and end date for Implementation**

HIPAA Implementation (Remediation)

Step 3 - Identification of Implementation Team

- **Assign responsibility to the project owner**
- **Assign personnel or outside resources**
- **Establish team reporting structure**

Step 4 - Implementation of Tasks

- **High GAP and Risk Task should be a priority**
- **Parallel Tasks**
- **Documenting HIPAA Implementation**
  - **Create Audit Trails**
  - **Creating Policy and Procedures**

Step 5 - Internal Certification

- **Affecting Changes to the Organization**
- **Roll Out of HIPAA Training Programs**

HIPAA Auditing and Maintenance Breakdown

- **Step 1 – Define the Scope of Audits**
- **Step 2 – Identify Frequency and Timeframes for Audits**
- **Step 3 – Identify Audit Team**
- **Step 4 – Developing Audit and Maintenance Plans**
- **Step 5 – Auditing and Maintenance Tasks**

HIPAA Auditing and Maintenance

- **Step 1 – Define the Scope of Audits**
  - **Define What to Audit**
  - **Define What is Not Audited**
  - **What Considerations are Made**
  - **What Assumptions are Made**
- **Step 2 –Identify the Frequency and Timeframes for Audits**
  - **Define When Should the Audit be Performed**
  - **Develop Audit Schedule**
- **Step 3 – Identify the Audit Team**
  - **Assign Responsibility**
  - **Establish a Team Reporting Structure**

HIPAA Auditing and Maintenance

- **Step 4 – Develop Audit and Maintenance Plans**
  - **EDI**
  - **Security**
  - **Business Continuity Plans**
  - **Privacy**
- **Step 5 – Auditing and Maintenance Tasks**
  - **Documentation of Audit GAP's (*changes*)**
  - **Identification of GAP's and Their Impact**
  - **Developing Strategies for Compliance**
  - **Developing Working Plans for Strategy Tasks**
  - **Implementation of Audit Strategies**
    - **Audit Tasks**
    - **Change Documentation**
    - **Propagating Changes**

For more information See our Booth or, contact:

Pat Sloan

1 - 888 – 392 - 2002

StoneHenge™

PARTNERS, INC.

PSLOAN@STONEHENGE.ORG

www.stonehenge.org